Judge Lauren King

UNITED STATES DISTRICT COURT

FOR THE WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

JASON GREGORIO, THOMAS VALENTINE, LEO MCGOWAN, VINCELLE CALICA, RAYMOND CALICA, AND TAMARA COWLES, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

GREEN DIAMOND RESOURCE COMPANY,

Defendant.

Case No. 2:24-cv-00596-LK

CONSOLIDATED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

Plaintiffs Jason Gregorio, Thomas Valentine, Leo McGowan, Vincelle Calica, Raymond Calica, and Tamara Cowles (collectively, "Plaintiffs"), individually and on behalf of all other similarly situated individuals, and by and through their undersigned counsel, file this Consolidated Class Action Complaint against Defendant Green Diamond Resource Company ("Green Diamond" or "Defendant") and allege the following based upon their personal knowledge of the facts, information and belief, and the investigation of their counsel.

I. INTRODUCTION

1. Plaintiffs bring this class action lawsuit against Green Diamond for its negligent failure to protect and safeguard Plaintiffs' and the Class's (approximately 27,896 individuals) highly sensitive personally identifiable information ("PII") culminating in a massive and preventable data breach (the "Data Breach" or "Breach"). As a result of Green Diamond's insufficient data security, cybercriminals easily infiltrated Green Diamond's inadequately protected computer systems and stole the PII of Plaintiffs and the Class and posted it on the dark web.[1]

2. Between June 26, 2023, and June 27, 2023, the unauthorized third-party had unfettered access to Plaintiffs' and the Class's highly sensitive PII where it was being inexplicably stored without sufficient data security and without sufficient oversight from Green Diamond.[2]

3. The confidential information exposed in the Data Breach includes Plaintiffs' and the Class's names, dates of birth, medical information, health insurance information, Social Security numbers, financial account information, driver's license numbers or state identification numbers, government-issued identification numbers, passport numbers, and full access

[1] *See* OFFICE OF THE MAINE ATTORNEY GENERAL, *Data Breach Notifications*, Green Diamond Resource Company, https://apps.web.maine.gov/online/aeviewer/ME/40/b85029fd-4eeb-4059-b381-65ffe99b1d93.shtml (last visited June 27, 2024).

[2] *Id.*

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

credentials.[3] Due to Green Diamond's negligence, Plaintiffs and the Class will face an imminent risk of identity theft and fraud for the rest of their lives.

4. Plaintiffs' and the Class's PII is undeniably in the hands of ill-intentioned cybercriminals. Shortly after the Data Breach, a well-known ransomware group, Akira, claimed responsibility for the Data Breach and claimed to have posted approximately 30GB of data stolen in the Breach on the dark web.[4]

Year	Month, Year	Company Affected	Industry	Sub-Industry	City/County	State	# Records Affected	Ransom Paid	Ransom Amount	Ransom Strain
2023	Jun, 2023	Green Diamond Resource Company	Business	Other	Seattle	Washington	27,896	Unknown	Unknown	Akira

5. Plaintiffs and Class Members have had their PII exposed as a result of Green Diamond's inadequately secured computer network. Green Diamond failed to uphold its data security obligations to Plaintiffs and Class Members by failing to properly safeguard and protect their PII, thereby enabling cybercriminals to steal such valuable and sensitive information.

6. For the rest of their lives, Plaintiffs and the Class Members will have to deal with the danger of identity thieves possessing and misusing their PII. Plaintiffs and Class Members will have to spend time responding to the Breach and are in immediate and heightened risk of identity theft as a direct and proximate result of the Data Breach. Plaintiffs and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their PII, and/or additional damages as described below.

---

[3] GREEN DIAMOND RESOURCE COMPANY, *Notice of Data Event* (April 19, 2024) https://www.greendiamond.com/dataevent.pdf (last visited June 27, 2024).

[4] *See* @compartitech, TWITTER (X) (Apr. 22, 2024, 5:10 AM), https://twitter.com/Comparitech/status/1782351310102069710; COMPARITECH, *Map of US Ransomware Attacks (updated daily)*, https://www.comparitech.com/ransomware-attack-map/.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

7. Plaintiffs bring this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

8. Plaintiff **Jason Gregorio** is domiciled in and is a citizen of the state of California. Plaintiff Gregorio received a Notice of Data Breach letter ("Notice Letter") from Green Diamond dated April 19, 2024, informing him that his name, Social Security number, date of birth, and full access credentials were accessed and/or acquired by an unauthorized person.[5]

9. Plaintiff **Thomas Valentine** is domiciled in and is a citizen of the State of Washington. Plaintiff Valentine received a Notice of Data Breach letter from Green Diamond dated April 19, 2024, informing him that his name, Social Security number, and date of birth were accessed and/or acquired by an unauthorized person.[6]

10. Plaintiff **Vincelle Calica** is domiciled in and is a citizen of the State of Washington. Plaintiff Vincelle Calica received a Notice of Data Breach letter from Green Diamond dated April 19, 2024, informing her that her name, Social Security number, and date of birth were accessed and/or acquired by an unauthorized person.[7]

11. Plaintiff **Raymond Calica** is domiciled in and is a citizen of the State of Washington. Plaintiff Raymond Calica received a Notice of Data Breach letter from Green

[5] *See* Ex. 1 (Notice Letter).

[6] *See* Ex. 2 (Notice Letter).

[7] *See* Ex. 3 (Notice Letter).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

Diamond dated April 19, 2024, informing him that his name, Social Security number, and date of birth were accessed and/or acquired by an unauthorized person.[8]

12. Plaintiff **Tamara Cowles** is domiciled in and is a citizen of the State of Washington. Plaintiff Cowles received a Notice of Data Breach letter from Green Diamond dated April 19, 2024, informing her that her name, Social Security number, and date of birth were accessed and/or acquired by an unauthorized person.[9]

13. Plaintiff **Leo McGowan** is domiciled in and is a citizen of the state of Georgia. Plaintiff McGowan received a Notice of Data Breach letter from Green Diamond dated April 19, 2024, informing him that his name, Social Security number, and data of birth were accessed and/or acquired by an unauthorized person.[10]

14. Defendant **Green Diamond Resource Company** is a Washington for Profit Corporation with its principal place of business located at 1301 5th Ave, suite 2700, Seattle, WA, 98101-2675. Green Diamond's Registered Agent is Galen G. Schuler, located at1301 5th Ave, suite 2700, Seattle, WA, 98101-2675.

III. JURISDICTION AND VENUE

15. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

[8] *See* Ex. 4 (Notice Letter).

[9] *See* Ex. 5 (Notice Letter).

[10] *See* Ex. 6 (Notice Letter).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

16. This Court has personal jurisdiction over Defendant because it is headquartered in and/or operates within this District and regularly transacts business, has agents, and is otherwise within this District.

17. Venue is likewise proper as to Defendant in this District because a substantial part of the events or omissions giving rise to the claim occurred in this District. 28 U.S.C. § 1391(b)(2).

IV. FACTUAL ALLEGATIONS

A. Green Diamond's Massive and Preventable Data Breach.

18. Green Diamond is a forest stewardship company that owns and manages working forests in nine (9) states throughout the western and southern United States.[11]

19. Green Diamond collected the PII of Plaintiffs and the Class for business and/or employment purposes.

20. By collecting the PII of Plaintiffs and the Class, Green Diamond undertook a duty to safeguard and protect such PII.

21. According to Green Diamond, on or about June 27, 2023, it became aware of suspicious activity in its computer network.[12]

22. After an investigation, Green Diamond determined that an unknown actor gained access to certain parts of its network between June 26, 2023, and June 27, 2023.

23. Green Diamond determined that the following types of PII were impacted by the Data Breach: names, dates of birth, medical information, health insurance information, Social Security numbers, financial account information, driver's license numbers or state identification

[11] *See* GREEN DIAMOND RESOURCE COMPANY, *About*, https://www.greendiamond.com/about/ (last visited June 27, 2024).

[12] *See* GREEN DIAMOND RESOURCE COMPANY, *Notice of Data Event* (April 19, 2024) https://www.greendiamond.com/dataevent.pdf (last visited June 27, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

numbers, government-issued identification numbers, passport numbers, and full access credentials.[13]

24. In other words, cybercriminals obtained everything they could possibly need to commit identity theft and fraud.

25. Despite learning of the Data Breach in June of 2023, Green Diamond waited until April of 2024 to notify victims of the Data Breach—***nearly one year later***.[14]

26. The Notice Letter obfuscated the nature of the Breach, stating "Green Diamond is notifying you out of an abundance of caution because although there is no evidence that information relating to you was actually seen by any unauthorized person, the investigation determined that certain information relating to you may have been accessed or acquired by an unknown unauthorized person."[15]

27. However, shortly after the Data Breach, a well-known ransomware group, Akira, claimed responsibility for the Data Breach, as pictured below:[16]

[IMAGE ON FOLLOWING PAGE]

[13] *Id.*

[14] *See, e.g.*, Exs. 1–6.

[15] *Id.*

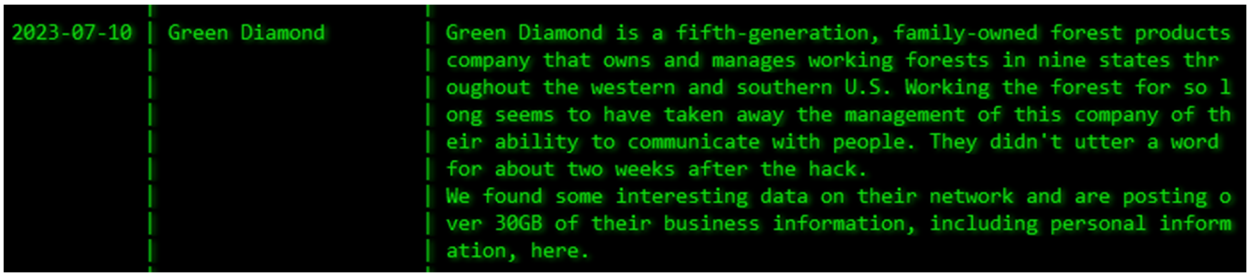
[16] @compartitech, TWITTER (X) (Apr. 22, 2024, 5:10 AM), https://twitter.com/Comparitech/status/1782351310102069710; RANSOMLOOK, *Green Diamond Resource*, https://www.ransomlook.io/group/Akira (last visited June 27, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

28. According to Akira, Green Diamond did not "utter a word for about two weeks after the hack."[17]

[17]@compartitech, TWITTER (X) (Apr. 22, 2024, 5:10 AM), https://twitter.com/Comparitech/status/1782351310102069710; RANSOMLOOK, *Green Diamond Resource*, https://www.ransomlook.io/group/Akira (last visited June 27, 2024).; @FalconFeeds.io, TWITTER (X) (July 11, 2023, 1:03 AM) https://twitter.com/FalconFeedsio/status/1678646129011957767/photo/1.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com



2023-07-10	Green Diamond	Green Diamond is a fifth-generation, family-owned forest products company that owns and manages working forests in nine states throughout the western and southern U.S. Working the forest for so long seems to have taken away the management of this company of their ability to communicate with people. They didn't utter a word for about two weeks after the hack. We found some interesting data on their network and are posting over 30GB of their business information, including personal information, here.

29. Akira posted over 30GB of data obtained in the Breach on its dark web portal.[18] However, Green Diamond's Notices to Plaintiffs and the Class failed to mention that Akira was the perpetrator responsible for the attack.

30. Trend Micro Research states, "Akira is swiftly becoming one of the fastest-growing ransomware families thanks to its use of double extortion tactics, a ransomware-as-a-service (RaaS) distribution model, and unique payment options."[19]

31. "Akira ransomware was first identified in May of 2023, and in less than a year, it has claimed at least 81 victims."[20]

32. "Akira leverages many common features for their targeting and operations. They operate as ransomware-as-a-service (RaaS), which is to say they focus on the ransomware operations, but partner with other cybercriminals for individual attacks and share the extorted fees. They also conduct double extortion; they steal sensitive data, deploy their ransomware, and then charge two fees. The first fee restores the encrypted systems, and the second fee ensures no leaks of stolen data. They are highly reliant on credential compromise as an infection vector, which

---

[18] *Id.*

[19] TREND MICRO, *Ransomware Spotlight Akira*, https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira (last visited June 27, 2024).

[20] OFFICE OF INFORMATION SECURITY, HC3 Analyst Note, Akira Ransomware (Feb. 7, 2024), https://www.hhs.gov/sites/default/files/akira-randsomware-analyst-note-feb2024.pdf (last visited June 27, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

provides them initial access into their target networks. Akira also operates a leak site where they publicly post information on their victims. Their targeting includes both Windows and Linux infrastructures, and while organizations in the United States are their focus, their targeting is global. They are also known to target the United Kingdom, Canada, Australia, New Zealand and other countries."[21]

33. "Officials from the FBI, Cybersecurity and Infrastructure Security Agency (CISA), Europol's European Cybercrime Centre (EC3), and the Netherlands' National Cyber Security Centre (NCSC-NL) published an advisory [] about [Akira], which has earned about $42 million in ransoms since emerging in March of 2023."[22]

34. "Akira ransomware actors have used known Cisco vulnerabilities like CVE-2020-3259 and CVE-2023-20269 to breach organizations through virtual private network (VPN) services that did not have multifactor authentication enabled."[23]

35. Akira is also known to use "use spear phishing campaigns and other tools to breach organizations. Once inside, they typically disable security software as a way to avoid detection while moving laterally."[24]

36. "According to the law enforcement agencies, the ransomware gang uses several different tools to exfiltrate data including FileZilla, WinRAR, AnyDesk and more. 'Akira threat actors do not leave an initial ransom demand or payment instructions on compromised networks, and do not relay this information until contacted by the victim,' the agencies said. 'Ransom

---

[21] *Id.*

[22] Jonathan Greig, *Akira ransomware gang made $42 million from 250 attacks since March 2023: FBI*, THE RECORD, (Apr. 18, 2024) https://therecord.media/akira-ransomware-attacked-hundreds-millions (last visited June 27, 2024).

[23] *Id.*

[24] *Id.*

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

payments are paid in Bitcoin to cryptocurrency wallet addresses provided by the threat actors. To further apply pressure, Akira threat actors threaten to publish exfiltrated data on the Tor network, and in some instances have called victimized companies, according to FBI reporting."'[25]

37. Altogether, Green Diamond utterly failed to take the necessary precautions required to safeguard and protect Plaintiffs' and the other Class Members' PII from unauthorized disclosure despite many warnings. Green Diamond's actions represent a flagrant disregard of the rights of the Class Members, both as to their privacy and their property.

B. Plaintiffs' Experiences.

Plaintiff Jason Gregorio's Experience

38. Plaintiff Gregorio received a Notice Letter from Green Diamond dated April 19, 2024, informing him that his name, Social Security number, date of birth, and full access credentials were accessed and/or acquired by an unauthorized person.

39. By soliciting and accepting Plaintiff Gregorio's PII, Green Diamond agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

40. Green Diamond was in possession of Plaintiff Gregorio's PII before, during, and after the Data Breach.

41. Following the Data Breach, Plaintiff Gregorio made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, enrolling in the credit monitoring services Green Diamond provided, reviewing and monitoring his accounts for fraudulent activity, and reviewing his credit reports. In total, Plaintiff Gregorio estimates he has spent over **five (5) hours** so far responding to the Data Breach.

42. Plaintiff Gregorio will be forced to expend additional time to review his credit

[25] *Id.*

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

reports and monitor his accounts for the rest of his life. This time, spent at Defendant's direction, has been lost forever and cannot be recaptured.

43. Plaintiff Gregorio places significant value in the security of his PII and does not readily disclose it. Plaintiff Gregorio entrusted Green Diamond with his PII with the understanding that Green Diamond would keep his information secured and would employ reasonable and adequate data security measures to ensure that his PII would not be compromised.

44. Plaintiff Gregorio has never knowingly transmitted unencrypted PII over the internet or any other unsecured sources.

45. As a direct and traceable result of the Data Breach, Plaintiff Gregorio suffered actual injury and damages after his PII was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his PII being accessed and stolen by cybercriminals; (c) loss of the benefit of his bargain because Green Diamond did not adequately protect his PII; (d) emotional distress because identity thieves now possess his first and last name paired with his Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII has been stolen and published on the dark web; (f) diminution in the value of his PII, a form of intangible property that Green Diamond obtained from Plaintiff Gregorio and/or his medical providers; and (g) other economic and non-economic harm.

46. Plaintiff Gregorio has been and will continue to be at a heightened and substantial risk of future identity theft and vulnerable to damages for ***years*** to come. This risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII stolen in the Data Breach.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

47. Plaintiff Gregorio has suffered great anxiety beyond mere worry because thieves intentionally targeted and stole his PII, including his Social Security number, which is now in the hands of cybercriminals. Specifically, Plaintiff Gregorio has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that his PII has been stolen.

48. Plaintiff Gregorio has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches. Absent Court intervention, Plaintiff Gregorio's PII will be wholly unprotected and at-risk of future data misuse.

Plaintiff Thomas Valentine's Experience

49. Plaintiff Valentine is a former customer of Green Diamond.

50. When Plaintiff first became a customer, Defendant required Plaintiff Valentine to provide substantial amounts of his PII.

51. Plaintiff Valentine received a Notice Letter from Green Diamond dated April 19, 2024, informing him that his name, Social Security Number, and date of birth were accessed and/or acquired by an unauthorized person.

52. The notice letter offered Plaintiff Valentine only one (1) year of credit monitoring services. One year of credit monitoring is not sufficient because Plaintiff Valentine now faces a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of his Private Information.

53. Plaintiff Valentine suffered actual injury in the form of time spent dealing with the Data Breach, monitoring his accounts for fraud, and mitigating the increased risk of fraud.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

54. Plaintiff Valentine would not have provided his Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its customers' personal information from theft, and that those systems were vulnerable to a breach.

55. Plaintiff Valentine suffered actual injury in the form of having his Private Information compromised and/or stolen as a result of the Data Breach.

56. Plaintiff Valentine suffered actual injury in the form of diminution in the value of his personal information – a form of intangible property that Plaintiff Valentine entrusted to Defendant and which was compromised in the Data Breach.

57. Plaintiff Valentine suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of cybercriminals.

58. Plaintiff Valentine has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

59. As a result of the Data Breach, Plaintiff Valentine made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options he will now need to use. Plaintiff Valentine has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

60. Plaintiff Valentine has suffered anxiety as a result of the release of his Private Information to cybercriminals, which he believed would be protected from unauthorized access and disclosure. This anxiety stems from unauthorized parties viewing, selling, and/or using his

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

Private Information for purposes of committing cyber and other crimes against him. Plaintiff Valentine is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud will have on his life.

61. Plaintiff Valentine also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Valentine; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

62. As a result of the Data Breach, Plaintiff Valentine anticipates spending considerable time and money on an ongoing basis to mitigate and address the many harms caused by the Data Breach.

Plaintiff Vincelle Calica's Experience

63. Plaintiff Vincelle Calica is a former employee of Green Diamond, and she provided her private information to Green Diamond as a condition of her employment.

64. Plaintiff Vincelle Calica reasonably understood and expected that Green Diamond would safeguard her Private Information, and that it would timely and adequately notify her in the event that there was a data breach affecting her Private Information. Plaintiff would not have allowed Green Diamond, or anyone in Green Diamond's position, to maintain or store her Private Information if she believed that Green Diamond would not implement reasonable industry standards to safeguard her Private Information from unauthorized access.

65. Plaintiff Vincelle Calica received a Notice Letter from Green Diamond dated April 19, 2024, informing her that her name, date of birth, Social Security number, financial account information, and full access credentials were accessed and/or acquired by an unauthorized person.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

66. In the notice letter, Green Diamond offered Plaintiff Vincelle Calica complimentary credit monitoring and identity theft protection through Transunion. Green Diamond also warned Plaintiff to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

67. Plaintiff Vincelle Calica greatly values her privacy and her Private Information. She takes reasonable steps to maintain the confidentiality of her Private Information, including not opening links or emails she does not recognize.

68. Plaintiff Vincelle Calica stores any and all documents containing her Private Information in secured locations.

69. Plaintiff Vincelle Calica has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: researching the Data Breach, reviewing her financial account statements for any indications of actual or attempted identity theft or fraud, and researching credit monitoring and identity theft protection services offered by Green Diamond.

70. Plaintiff Vincelle Calica has spent at least 20 hours dealing with the Data Breach to date, valuable time she otherwise would have spent on other activities.

71. As a result of the Data Breach, Plaintiff Vincelle Calica has suffered emotional distress from the release of her Private Information including anxiety about unauthorized parties viewing, selling, and/or using her personal information for purposes of identity theft and fraud. Plaintiff Vincelle Calica remains very concerned about identity theft and fraud as well as the consequences of such identity theft and fraud resulting from the Data Breach.

72. Plaintiff Vincelle Calica has suffered actual injury from having her Private Information compromised including but not limited to: (a) damage to and diminution in the value

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

of her PII, a form of property that Green Diamond obtained from Plaintiff Vincelle Calica; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

73. As a result of the Data Breach, Plaintiff Vincelle Calica anticipates spending considerable time and money on an ongoing basis to mitigate and address harm caused by the Data Breach.

74. Plaintiff Vincelle Calica is also at present and future increased risk of identity theft and fraud.

Plaintiff Raymond Calica's Experience

75. Plaintiff Raymond Calica is a former contractor for, and labor negotiator with, Green Diamond and provided his private information to Green Diamond as a condition of his employment.

76. Plaintiff Raymond Calica reasonably understood and expected that Green Diamond would safeguard his Private Information, and that it would timely and adequately notify him in the event that there was a data breach affecting his Private Information. Plaintiff would not have entrusted Green Diamond, or anyone in Green Diamond's position, with his Private Information if he believed that Green Diamond would not implement reasonable industry standards to safeguard his Private Information from unauthorized access.

77. Plaintiff Raymond Calica received a Notice Letter from Green Diamond dated April 19, 2024, informing him that his name, date of birth, and Social Security number were accessed and/or acquired by an unauthorized person.

78. In the notice letter, Green Diamond offered Plaintiff Raymond Calica complimentary credit monitoring and identity theft protection through Transunion. Green

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

Diamond also warned Plaintiff to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

79. Plaintiff Raymond Calica greatly values his privacy and his Private Information. He takes reasonable steps to maintain the confidentiality of his Private Information, including not opening links or emails he does not recognize.

80. Plaintiff Raymond Calica stores any and all documents containing Private Information in a secured location.

81. Plaintiff Raymond Calica has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: researching the Data Breach, reviewing his financial account statements for any indications of actual or attempted identity theft or fraud, and researching credit monitoring and identity theft protection services offered by Green Diamond.

82. Plaintiff Raymond Calica has spent at least 2 hours dealing with the Data Breach to date, valuable time he otherwise would have spent on other activities.

83. As a result of the Data Breach, Plaintiff Raymond Calica has suffered emotional distress from the release of his Private Information, including anxiety about unauthorized parties viewing, selling, and/or using his personal information for purposes of identity theft and fraud. Plaintiff Raymond Calica remains very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

84. Plaintiff Raymond Calica suffered actual injury from having his Private Information compromised as a result of the Data Breach, including but not limited to: (a) damage to and diminution in the value of his PII, a form of property that Green Diamond obtained from

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

Plaintiff Raymond Calica; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

85. As a result of the Data Breach, Plaintiff Raymond Calica anticipates spending considerable time and money on an ongoing basis to mitigate and address harm caused by the Data Breach.

Plaintiff Tamara Cowles' Experience

86. Plaintiff Tamara Cowles is a former employee of Green Diamond and provided her private information to Green Diamond as a condition of her employment.

87. Plaintiff Cowles reasonably understood and expected that Green Diamond would safeguard her Private Information, and that it would timely and adequately notify her in the event that there was a data breach affecting her Private Information. Plaintiff would not have entrusted Green Diamond, or anyone in Green Diamond's position, with her Private Information if she believed that Green Diamond would not implement reasonable industry standards to safeguard her Private Information from unauthorized access.

88. Plaintiff Cowles received a Notice Letter from Green Diamond dated April 19, 2024, informing her that her name, date of birth, Social Security number, and full access credentials were accessed and/or acquired by an unauthorized person.

89. In its notice letter, Green Diamond offered Plaintiff Cowles complimentary credit monitoring and identity theft protection through Transunion. Green Diamond also warned Plaintiff Cowles to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

90. Plaintiff Cowles greatly values her privacy and her Private Information. She takes reasonable steps to maintain the confidentiality of her Private Information, including not opening links or emails she does not recognize.

91. Plaintiff Cowles stores any and all documents containing Private Information in a secured location.

92. Plaintiff Cowles has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to: researching the data breach, reviewing her financial account statements for any indications of actual or attempted identity theft or fraud, and researching credit monitoring and identity theft protection services offered by Green Diamond.

93. Plaintiff Cowles has spent several hours dealing with the Data Breach to date, valuable time she otherwise would have spent on other activities.

94. As a result of the Data Breach, Plaintiff Cowles has suffered emotional distress due from the release of her Private Information including anxiety about unauthorized parties viewing, selling, and/or using her personal information for purposes of identity theft and fraud. Plaintiff Cowles remains exceptionally concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

95. Plaintiff Cowles suffered actual injury from having her Private Information compromised as a result of the data breach, including but not limited to: (a) damage to and diminution in the value of her PII, a form of property that Green Diamond obtained from Plaintiff Cowles; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

96. As a result of the Data Breach, Plaintiff Cowles anticipates spending considerable time and money on an ongoing basis to mitigate and address harm caused by the Data Breach.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

97. As a result of the Data Breach, Plaintiff Cowles is at present and future increased risk of identity theft and fraud.

Plaintiff Leo McGowan's Experience

98. Plaintiff McGowan received a Notice Letter from Green Diamond dated April 19, 2024, informing him that his name, Social Security number, and date of birth were accessed and/or acquired by an unauthorized person.

99. By soliciting and accepting Plaintiff McGowan's PII, Green Diamond agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

100. Green Diamond was in possession of Plaintiff McGowan's PII before, during, and after the Data Breach.

101. Following the Data Breach, Plaintiff McGowan made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, and reviewing his credit reports.

102. Plaintiff McGowan will be forced to expend additional time to review his credit reports and monitor his accounts for the rest of his life. This is time, spent at Defendant's direction, which has been lost forever and cannot be recaptured.

103. Plaintiff McGowan places significant value in the security of his PII and does not readily disclose it. Plaintiff McGowan entrusted Green Diamond with his PII with the understanding that Green Diamond would keep his information secure and would employ reasonable and adequate data security measures to ensure that his PII would not be compromised.

104. Plaintiff McGowan has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

105. As a direct and traceable result of the Data Breach, Plaintiff McGowan suffered

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

actual injury and damages after his PII was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his PII being accessed and stolen by cybercriminals; (c) loss of the benefit of his bargain because Green Diamond did not adequately protect his PII; (d) emotional distress because identity thieves now possess his first and last name paired with his Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII has been stolen and published on the dark web; (f) diminution in the value of his PII, a form of intangible property that Green Diamond obtained; and (g) other economic and non-economic harm.

106. Following the Breach, Plaintiff McGowan suffered a decrease in his credit score.

107. Also following the Breach, Plaintiff McGowan was forced to change his Amazon account password after he discovered that the name on his account was changed without his authorization.

108. Finally, Plaintiff McGowan has experienced an enormous increase in spam calls following the Data Breach. On information and belief, Plaintiff's phone was compromised as a result of the Data Breach, as cybercriminals are able to use an individual's PII that is accessible on the dark web, as Plaintiff's is here, to gather and steal even more information.[26]

109. Plaintiff McGowan has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for ***years*** to come. This risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII stolen in the Data Breach.

[26] What do Hackers do with Stolen Information, AURA, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited June 17, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

110. Knowing that thieves intentionally targeted and stole his PII, and knowing that his PII, including his Social Security number, is now in the hands of cybercriminals has caused Plaintiff McGowan great anxiety beyond mere worry. Specifically, Plaintiff McGowan has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that his PII has been stolen.

111. Plaintiff McGowan has a continuing interest in ensuring that his PII, which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches. Absent Court intervention, Plaintiff McGowan's PII will be wholly unprotected and at-risk of future data breaches.

C. Cybercriminals Will Use the PII Obtained in the Breach to Defraud Plaintiffs and the Class.

110. PII is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of sordid ways for criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune, including ways already experienced by Plaintiffs as set forth above.

111. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[27] For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during

[27] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last visited June 11, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

arrests, and many other harmful forms of identity theft.[28] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and the Class Members.

112. Social Security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[29]
>
> (Emphasis added.)

113. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years to come.[30]

114. There is no doubt this was a financially motivated breach, as the only reason Akira would go through the trouble of running a targeted cyberattack against a company like Green Diamond is to get information that it can monetize by selling on the black market for use in the kinds of criminal activity described herein. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[31] "[I]f there is reason to believe that

---

[28] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ 9last visited June 11, 2024).

[29] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited June 11, 2024).

[30] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu (last visited June 11, 2024).

[31] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web (last visited June 11, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

your personal information has been stolen, you should assume that it can end up for sale on the dark web."[32]

115. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, they ***will*** use it.[33]

116. Hackers may not have immediate use of the information, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information ***may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[34]

117. For instance, with a stolen Social Security number, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[35]

118. The ramifications of Defendant's failure to keep Class Members' PII secure are long lasting and severe. Once that information is stolen and compromised, fraudulent use of that

---

[32] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited June 11, 2024).

[33] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info (last visited June 11, 2024).

[34] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu (last visited June 11, 2024).

[35] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited June 11, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

information and damage to victims may continue for years. Fraudulent activity might not show up for six to twelve months or even longer.

119. Further, criminals often trade stolen PII on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

120. Approximately 21% of victims do not realize that their identify has been compromised until more than two years after it has happened. [36] This gives thieves ample time to seek multiple medical treatments under the victim's name, among other misuses. 40% percent of consumers found out they were a victim of medical identity theft only after they received collection letters from creditors for expenses that were incurred under their names.[37]

121. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit and protecting themselves in the future.[38]

122. As a direct and proximate result of the Data Breach, Plaintiffs and the Class have had their PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of further harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and

---

[36] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2.

[37] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), *available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited June 11, 2024).

[38] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last visited June 11, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiffs and other Class Members must go through, which can include spending countless hours filing police reports, following Federal Trade Commission checklists, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps.

123. Plaintiffs and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;

b. Trespass, damage to, and theft of their personal property including PII;

c. Improper exposure of their PII;

d. Online publication of their PII like the dark web;

e. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and misused;

f. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their PII and that identity thieves have already used that information to defraud other victims of the Data Breach;

g. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

h. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

i. Ascertainable losses in the form of deprivation of the value of Plaintiffs' and Class Members' personal information for which there is a well-established and quantifiable national and international market;

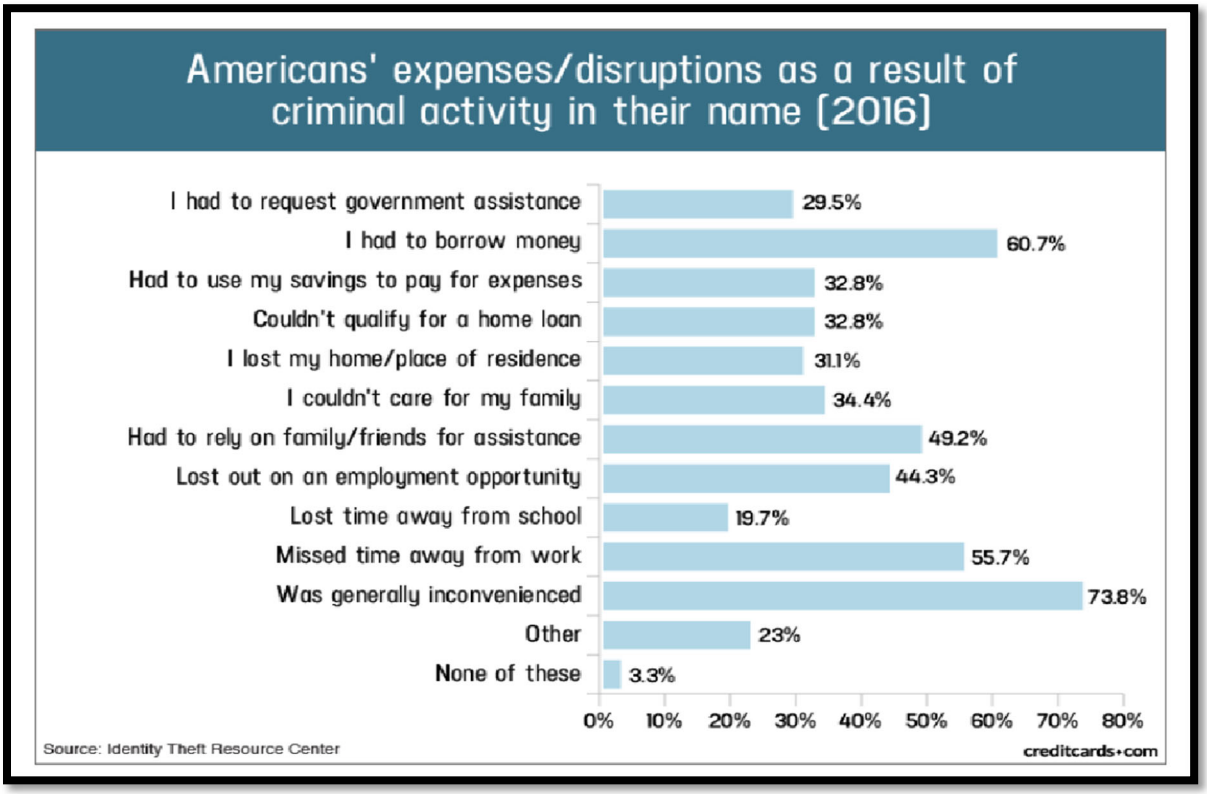
j. The loss of use and access to their credit, accounts, and/or funds;

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

k. Damage to their credit due to fraudulent use of their PII; and

l. Increased cost of financing loans, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

124. Below is a chart that shows the kinds of expenses and disruptions that victims of identity theft experience[39]:



125. Moreover, Plaintiffs and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiffs' PII.

[39] Jason Steele, *Credit Card and ID Theft Statistics*, CREDITCARDS.COM (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

126. Plaintiffs and Class Members also have an interest in ensuring that their PII that was provided to Green Diamond is removed from Green Diamond's unencrypted files.

127. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiffs and Class Members an inadequate 12 or 24 months of identity theft repair and monitoring services.[40] This limited identity theft monitoring is, however, insufficient to protect Plaintiffs and Class Members from a lifetime of identity theft risk.

128. Defendant further acknowledged, in its breach notification letter, that, in response to the Data Breach, Green Diamond is "reviewing existing security policies and implemented additional cybersecurity measures to further protect against similar incidents moving forward."[41] Green Diamond should have implemented these additional cybersecurity measures before the Data Breach.

129. The notice letters further acknowledged that the Data Breach would cause additional inconveniences, including financial harm, to affected individuals and provided numerous actions Class Members could take to mitigate those harms caused by the Data Breach. Green Diamond's notice letter states: "We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."[42]

130. At Green Diamond's suggestion, Plaintiffs are desperately trying to mitigate the damage that Green Diamond has caused them. Given the kind of PII hackers stole from Green Diamond's network, however, Plaintiffs are certain to incur additional damages. Because identity

[40] *See* Exs. 1–6.

[41] *Id.*

[42] *Id.*

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

thieves have obtained confidential PII, Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and tedious process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[43]

131. None of this should have happened, the Data Breach was preventable.

D. Defendant was Aware of the Risk of Cyber Attacks.

132. Data security breaches have dominated the headlines for the last two decades, and it does not take an IT industry expert to know it. The general public is aware of some of the biggest cybersecurity breaches including Target,[44] Yahoo,[45] Marriott International,[46] Chipotle, Chili's, Arby's,[47] and others.[48]

133. Green Diamond knew or should have known that it was at risk for a data breach that could expose the PII it collected and maintained.

---

[43] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

[44] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/ (last visited June 11, 2024).

[45] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html (last visited June 11, 2024).

[46] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ (last visited June 11, 2024).

[47] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b (last visited June 11, 2024).

[48] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (last visited June 11, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

134. It is well-publicized and well-known that Akira targets businesses similar to Green Diamond.[49]

135. "'The Akira ransomware gang has infiltrated and impacted more than 250 organizations over the last year and continues to attack a "wide range of businesses and critical infrastructure entities in North America, Europe, and Australia,' the FBI and European law enforcement agencies warned[.]"[50]

136. "The ransomware gang has claimed a steady stream of incidents in 2024, including an attack on prominent cloud hosting services provider Tietoevry."[51]

137. Green Diamond was clearly aware of the risks and the harm that could result from inadequate date security but failed to implement appropriate data security measures.

E. Defendant Could Have Prevented the Data Breach.

138. Data breaches are preventable.[52] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[53] She added that "[o]rganizations that collect, use, store, and share sensitive

---

[49] *See* https://thehackernews.com/2024/04/akira-ransomware-gang-extorts-42.html; https://thehackernews.com/2024/04/akira-ransomware-gang-extorts-42.html (last visited June 11, 2024).

[50] Jonathan Greig, *Akira ransomware gang made $42 million from 250 attacks since March 2023: FBI*, THE RECORD, (Apr. 18, 2024) https://therecord.media/akira-ransomware-attacked-hundreds-millions (last visited June 27, 2024).

[51] *Id.*

[52] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[53] *Id.* at 17.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

personal data must accept responsibility for protecting the information and ensuring that it is not compromised…"[54]

139. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures… Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[55]

140. In a Data Breach like the one here, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The guidelines also emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[56] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

141. Upon information and belief, Green Diamond failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including those in the FTC's guidelines. Green Diamond also failed to meet the minimum standards of any of the following

---

[54] *Id.* at 28.

[55] *Id.*

[56] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 11, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in cybersecurity readiness.

142. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[57]

143. To prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Since end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices, and use a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege. No users should be assigned administrative access unless absolutely needed,

[57] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited June 11, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have wide access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if not in use.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policies.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[58]

144. Further, to prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the

[58] *Id.* at 3–4.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)…

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[59]

145. In addition, to prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**

  - Apply the latest security updates.
  - Use threat and vulnerability management systems.
  - Perform regular audits and remove privileged credentials.

- **Thoroughly investigate and remediate alerts**

[59] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

- Prioritize and treat commodity malware infections as full potential compromises.

- **Include IT Pros in security discussions**

  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely.

- **Build credential hygiene**

  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords.

- **Apply principle of least-privilege**

  - Monitor for adversarial activities.
  - Hunt for brute force attempts.
  - Monitor for cleanup of Event Logs.
  - Analyze logon events.

- **Harden infrastructure**

  - Use Windows Defender Firewall.
  - Enable tamper protection.
  - Enable cloud-delivered protection.
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[60]

146. Since Defendant stored the PII of many individuals through the course of its business, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

[60] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited June 11, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

147. Specifically, among other failures, Green Diamond had vast amounts of unencrypted confidential information in its systems. Such PII should have been segregated and protected by an encrypted system.[61]

148. In sum, this Data Breach could have skillfully been prevented using industry standard network segmentation procedures and encrypting all confidential information. Further, the Data Breach could have been prevented if Defendant utilized appropriate malware prevention and detection technologies.

149. Green Diamond was negligent in its failure to ensure it had proper security measures in place to store Plaintiffs' and Class Members' confidential PII.

F. Defendant's Response to the Data Breach is Inadequate.

150. Defendant failed to timely inform Plaintiffs and Class Members of the Data Breach to adequately protect themselves from identity theft.

151. Defendant stated that the Data Breach was discovered around June of 2023—almost a full year before Defendant notified Plaintiffs and the Class of the incident. Defendant failed to inform Plaintiffs and Class Members exactly what information was exposed in the Data Breach and who carried out the Breach, leaving Plaintiffs and Class Members unsure as to the scope of information that was compromised and the dangers they faced.

152. If Green Diamond had investigated the Data Breach more diligently and reported it sooner, Plaintiffs and the Class could have taken steps to protect themselves and mitigate the harm suffered by the Breach.

V. CLASS ACTION ALLEGATIONS

[61] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption (last visited June 11, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

153. Plaintiffs incorporate by reference all preceding paragraphs as if fully restated herein.

154. Plaintiffs bring this action individually and on behalf of all members of the following class of similarly situated persons (collectively, the "Class or "Class Member") against Green Diamon, pursuant to Federal Rule of Civil Procedure 23:

> **Nationwide Class**
> All persons residing in the United States who received a Notice Letter from Green Diamond and had their PII compromised by an unknown third-party cybercriminal as a result of the Data Breach that occurred in or around June of 2023.
>
> **California Subclass**
> All persons residing in California whose PII was compromised as a result of the Data Breach.
>
> **Washington Subclass**
> All residents in the State of Washington whose PII was compromised as a result of the Data Breach.

Excluded from the Class is Defendant, any entity in which Defendant has a controlling interest, Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

155. Plaintiffs reserve the right to amend the above definitions or to propose additional subclasses in subsequent pleadings and motions for class certification.

156. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

157. **Numerosity:** Upon knowledge and belief, there are approximately 27,896 Members of the proposed Class and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Green Diamon's own records.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

158. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class. All Class Members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class Members in the same manner.

159. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the other Class Members they seek to represent; Plaintiffs have retained counsel competent and highly experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

160. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. No unusual difficulties are likely to be encountered in the management of this matter as a class action. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Green Diamond's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

161. **Commonality and Predominance:** Common questions of law and fact exist as to all proposed Class members and predominate over questions affecting only individual Class Members. These common questions include:

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant's inadequate data security measures were a cause of the Data Breach;

c. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's PII;

d. Whether Defendant owed a legal duty to Plaintiffs and the other Class Members to exercise due care in collecting, storing, and safeguarding their PII;

e. Whether Defendant negligently or recklessly breached their legal duties owed to Plaintiffs and the Class Members to exercise due care in collecting, storing, and safeguarding their PII;

f. Whether Defendant failed to provide adequate cyber security;

g. Whether Defendant knew or should have known that its computer and network security systems were vulnerable to cyber attacks;

h. Whether Defendant's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its company network;

i. Whether Defendant was negligent in permitting unencrypted PII of vast numbers of individuals to be stored within its network;

j. Whether Defendant was negligent in permitting unencrypted PII of vast numbers of individuals to be stored within its network;

k. Whether Defendant was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach to include former employees, applicants, and business associates;

l. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

m. Whether Defendant continues to breach duties to Plaintiffs and the Class;

n. Whether Plaintiffs and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

o. Whether Plaintiffs and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and

p. Whether Defendant's actions alleged herein constitute gross negligence, and whether Plaintiffs and Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of all Plaintiffs, the Nationwide Class, and the California and Washington Subclasses)

162. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

163. Defendant Green Diamond solicited, gathered, and stored the PII of Plaintiffs and the Class.

164. Defendant had full knowledge of the sensitivity of the PII it maintained and of the types of harm that Plaintiffs and Class Members could and would suffer if their PII were wrongfully disclosed. Defendant had a duty to Plaintiffs and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiffs and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

and the Class Members had no ability to protect their PII that was in Green Diamond's possession. As such, a special relationship existed between Green Diamond and the Plaintiffs and the Class.

165. Defendant was well aware of the fact that cybercriminals routinely target organizations through cyberattacks in an attempt to steal the collected PII.

166. Defendant owed Plaintiffs and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing PII, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

167. Defendant's duties extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

168. Defendant had the duty to protect and safeguard the PII of Plaintiffs and the Class from being vulnerable to cyberattacks by encrypting documents containing PII, by not permitting documents containing unencrypted PII to be maintained on its systems, and other similarly common-sense precautions when dealing with sensitive PII. Additional duties that Green Diamond owed Plaintiffs and the Class include:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;

b. To protect the PII in its possession using reasonable and adequate security procedures and systems;

c. To adequately and properly audit and routinely test its systems;

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

d. To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

e. To adequately and properly audit, test, and train its employees regarding how to avoid phishing attempts and scams;

f. To train its employees not to store PII for longer than necessary;

g. To implement processes to quickly detect a data breach, security incident, or intrusion; and

h. To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

169. Plaintiffs and the Class were the intended beneficiaries of Defendant's duties, creating special relationships between them and Green Diamond. Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiffs and the Class had entrusted to it.

170. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;

b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to employe systems to protect against malware;

d. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII, including maintaining it in an encrypted format;

e. Failing to adequately and properly audit, test, and train its employees regarding how to avoid phishing attempts and scams

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

f. Failing to consistently enforce security policies aimed at protecting Plaintiffs and the Class's PII;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

h. Failing to abide by reasonable retention and destruction policies for PII it collects and stores; and

i. Failing to promptly and accurately notify Plaintiffs and Class Members of the Data Breach that affected their PII.

171. Defendant's willful failures to abide by these duties were wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

172. As a direct and proximate result of Defendant's grossly negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harm and damages (as alleged above).

173. The damages Plaintiffs and the Class have suffered (as alleged above) were and are reasonably foreseeable.

174. The damages Plaintiffs and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

175. Plaintiffs and the Class have suffered injury, including as described above, and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION

NEGLIGENCE PER SE

(On Behalf of all Plaintiffs, the Nationwide Class, and the California Subclass)

176. Plaintiffs restate and reallege the allegations in paragraphs of the proceeding factual allegations above as if fully set forth herein.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

177. Pursuant to Section 5 of the FTCA, Green Diamond had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

178. Green Diamond breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

179. Plaintiffs and Class Members are within the class of persons that the FTCA is intended to protect.

180. Section 5 of the FTCA Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC publications and orders, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Green Diamond's duty.

181. Green Diamond violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

182. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Green Diamond's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

183. Green Diamond's violations of the FTCA constitute *Negligence Per Se*.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

184. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to Green Diamond's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

185. As a direct and proximate result of Green Diamond's *Negligence Per Se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

186. Green Diamond breached its duties to Plaintiffs and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

187. As a direct and proximate result of Green Diamond's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

188. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Green Diamond to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of all Plaintiffs, the Nationwide Class, and the California and Washington Subclasses)

189. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

190. Through the use of Plaintiffs' and Class Members' PII, Defendant received monetary benefits.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

191. Defendant collected, maintained, and stored the PII of Plaintiffs and Class Members and, as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiffs and Class Members.

192. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiffs and Class Members and accepted that monetary benefit.

193. However, acceptance of the benefit under the facts and circumstances described herein, make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Green Diamond instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper and ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

194. Under the principle of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members because Green Diamond failed to implement the appropriate data management and security measures, and Green Diamond failed to ensure the appropriate data management and security measures were in place.

195. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

196. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to allow Defendant to have or maintain their PII.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

197. As a direct and proximate result of Green Diamond's decision to profit rather than provide adequate data security, and as a direct and proximate cause of Green Diamond's failure to ensure it provided adequate data security, Plaintiffs and Class Members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Green Diamond reasonably should have expended on data security measures to secure Plaintiffs' PII, (ii) time and expenses mitigating harms, (iii) diminished value of the PII, (iv) harms as a result of identity theft; and (v) an increased risk of future identity theft.

198. Defendant, upon information and belief, has therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiffs and the Class in direct violation of Plaintiffs' and Class Members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

199. Accordingly, Plaintiffs and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiffs and the Class.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of all Plaintiffs, the Nationwide Class, and the California and Washington Subclasses)

200. Plaintiffs incorporate by reference all allegations of the preceding factual allegations as though fully set forth herein.

201. Defendant required Plaintiffs and Class Members to provide their PII. In exchange, Defendant entered into implied contracts with Plaintiffs and Class Members in which Defendant

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

agreed to comply with its statutory and common law duties to protect Plaintiffs' and Class Members' PII and to timely notify them in the event of a data breach.

202. Plaintiffs and Class Members would not have provided their PII to Defendant had they known that Defendant would not adequately safeguard their PII, as promised, or provide timely notice of a Data Breach.

203. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendant.

204. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

205. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class Members.

FIFTH CAUSE OF ACTION
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL")
Cal. Bus. & Prof. Code §§ 17200 – 17210
(On Behalf of all Plaintiffs, the Nationwide Class, and the California Subclass)

206. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

207. Plaintiff Gregorio brings this Count on his own behalf and on behalf of the California Subclass and is referred to as "Plaintiff" throughout this section.

208. Defendant is a "person" defined by Cal. Bus. & Prof. Code § 17201.

209. Defendant violated Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

210. In the course of conducting its business, Defendant committed "unlawful" business practices by, *inter alia*, failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII, and by violating the statutory and common law alleged herein, including, *inter alia*, the California Consumer Privacy Act of 2018 (Cal. Civ. Code § 1798.100, *et seq.*), Cal. Civil Code § 1798.81.5, Cal. Civ. Code § 1798.80 *et seq.*, and Section 5 of the FTC Act. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, and want of ordinary care are ongoing and continue to this date.

211. Defendant also violated the UCL by failing to timely notify Plaintiff and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiff and Class Members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII and identities.

212. Defendant violated the unfair prong of the UCL by establishing the sub-standard security practices and procedures described herein and storing Plaintiff's and Class Members' PII in an unsecure, internet accessible, electronic environment. Specific failures to follow industry standards and exercise reasonable care include: failing to encrypt the PII accessed during the Data Breach; maintaining PII for longer than it has a legitimate use; failing to regularly update passwords; failure to implement two-factor authentication for access to accounts and systems containing PII; failing to adequately train employees to recognize phishing and other social engineering techniques; and failing to implement and use software that can adequately detect phishing emails. These unfair acts and practices were immoral, unethical, oppressive,

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class Members. The harm these practices caused to Plaintiff and Class Members outweighed their utility, if any.

213. Defendant's above-described wrongful actions, inaction, want of ordinary care, and practices also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant's practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, CRA, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

214. Defendant engaged in unfair business practices under the "balancing test." The harm caused by Defendant's failure to implement proper data security measures, as described in detail above, greatly outweighs any perceived utility. Indeed, Defendant's failure to follow basic data security protocols cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiff and Class Members, directly causing the harms alleged.

215. Defendant engaged in unfair business practices under the "tethering test." Defendant's failure to implement proper data security measures, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.,* Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

216. Defendant engaged in unfair business practices under the "FTC test." The harm caused by Defendant's failure to implement proper data security measures, as described in detail above, is substantial in that it affects thousands of Class Members and has caused those persons to suffer actual harms. This harm continues given the fact that Plaintiff's and California Subclass members' PII remains in Defendant's possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendant's actions and omissions violated Section 5(a) of the Federal Trade Commission Act. *See* 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); *see also, e.g., In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

217. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class Members' were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value and the right to control their personal information.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

218. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

219. Plaintiff and California Subclass Members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

220. By deceptively storing, collecting, and disclosing their personal information, Defendant has taken money or property from Plaintiff and California Subclass Members.

221. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and Class Members' rights.

222. Plaintiff and California Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

SIXTH CAUSE OF ACTION
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code §§ 1798.100 et seq., § 1798.150(a)
(On Behalf of Plaintiff Gregorio and the California Subclass)

223. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged herein.

224. Plaintiff Gregorio brings this Count on his own behalf and on behalf of the California Subclass and is referred to as "Plaintiff" throughout this section.

225. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides: "Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following: (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. (B) Injunctive or declaratory relief. (C) Any other relief the court deems proper.

226. Defendant is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of $25 million.

227. Plaintiff and California Subclass Members are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

228. The personal information of Plaintiff and the California Subclass Members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

229. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the California Subclass Members' personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass Members. Specifically, Defendant subjected Plaintiff's and the California Subclass Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

230. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and California Subclass Members' personal information included exfiltration, theft, or disclosure through Defendant's servers, systems, and website, and/or the dark web, where hackers further disclosed the personal identifying information alleged herein.

231. As a direct and proximate result of Defendant's acts, Plaintiff and the California Subclass Members were injured and lost money or property, including but not limited to the loss of Plaintiff's and California Subclass Members' legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

232. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages."

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

233. Accordingly, Plaintiff and the California Subclass Members by way of this complaint seek actual pecuniary damages suffered as a result of Defendant's violations described herein.

234. Plaintiff provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). This written notice was received by Green Diamond on May 9, 2024. Defendant failed to respond and did not cure the violation within 30 days thereof. Therefore, Plaintiff seeks all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750.00) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

SEVENTH CAUSE OF ACTION
VIOLATION OF THE CALIFORNIA CONSUMER RECORDS ACT, Cal. Civ. Code §§ 1798.80 *et seq.* (On Behalf of Plaintiff Gregorio and the California Subclass)

235. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged herein.

236. Plaintiff Gregorio brings this Count on his own behalf and on behalf of the California Subclass and is referred to as "Plaintiff" throughout this section.

237. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

238. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

239. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

240. Plaintiff and the California Subclass Members are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Defendant for the purpose of obtaining a product and/or service, via their employment with Defendant's clients, from Defendant.

241. The personal information of Plaintiff and the California Subclass Members at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

242. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Plaintiff's and California Subclass Members' personal information and that the risk of a data breach or theft was highly likely. Defendant failed to

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass Members. Specifically, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiff and the California Subclass Members from unauthorized access, destruction, use, modification, or disclosure. Defendant further subjected Plaintiff's and the California Subclass Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

243. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiff and the California Subclass Members included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and the California Subclass Members by the cyber attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

244. As a direct and proximate result of Defendant's acts or omissions, Plaintiff and the California Subclass Members were injured and lost money or property including, but not limited to, the loss of Plaintiff's and the California Subclass Members' legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

245. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

246. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

a) The name and contact information of the reporting person or business subject to this section;

b) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c) If the information is possible to determine at the time the notice is provided, then any of the following:

   i. the date of the breach,

   ii. the estimated date of the breach, or

   iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

d) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e) A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

f) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

247. Defendant failed to provide the legally compliant notice under § 1798.82(d) to Plaintiff and members of the California Subclass. On information and belief, to date, Defendant has not sent written notice of the data breach to all impacted individuals. As a result, Defendant has violated § 1798.82 by not providing legally compliant and timely notice to all California Subclass Members. Because not all members of the class have been notified of the breach, members could have taken action to protect their personal information, but were unable to do so because they were not timely notified of the breach.

248. Defendant failed to provide the legally compliant notice under § 1798.82(d) to Plaintiff and members of the California Subclass. On information and belief, to date, Defendant has not sent written notice of the data breach to all impacted individuals. As a result, Defendant has violated § 1798.82 by not providing legally compliant and timely notice to all California Subclass Members. Because not all members of the class have been notified of the breach, members could have taken action to protect their personal information, but were unable to do so because they were not timely notified of the breach.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

249. On information and belief, many California Subclass Members affected by the breach have not received any notice at all from Defendant in violation of Section 1798.82(d).

250. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and California Subclass Members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

251. As a direct consequence of the actions as identified above, Plaintiff and California Subclass Members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

EIGHTH CAUSE OF ACTION
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT
(On Behalf of all Plaintiffs, the Nationwide Class, and the Washington Subclass)

252. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged herein.

253. Plaintiff Valentine brings this Count on his own behalf and on behalf of the Washington Subclass.

254. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

255. Defendant is a "person" as described in RWC 19.86.010(1).

256. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

257. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

258. In the course of conducting its business, Defendant committed "unfair or deceptive acts or practices" by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Washington Subclass Members' PII, and violating the common law alleged herein in the process. Plaintiff and Washington Subclass Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

259. Defendant also violated the CPA by failing to timely notify and concealing from Plaintiff and Washington Subclass Members information regarding the unauthorized release and disclosure of their PII. If Plaintiff and Washington Subclass Members had been notified in an appropriate fashion of Defendant's CPA violations, rather than having this information hidden

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

from them, they could have taken precautions to safeguard and protect their PII, medical information, and identities.

260. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendant's wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

261. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonable available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

262. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the CPA, Plaintiff and Washington Subclass Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of their PII; (5) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

263. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of himself and the Washington Subclass, seeks restitution and an injunction prohibiting Defendant

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

from continuing such wrongful conduct, and requiring Defendant to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it.

264. Plaintiff, on behalf of himself and Washington Subclass Members, also seeks to recover actual damages sustained by each Washington Subclass Member, together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiff and Washington Subclass Members request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Washington Subclass Member by three times the actual damages sustained, not to exceed $25,000.00 per Washington Subclass Member.

NINTH CAUSE OF ACTION
INJUNCTIVE AND DECLARATORY RELIEF
(On Behalf of all Plaintiffs, the Nationwide Class, and the California and Washington Subclasses)

265. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

266. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

267. As previously alleged and pleaded, Defendant owed duties of care to Plaintiffs and Class Members that required it to adequately secure their PII.

268. Defendant still possesses the PII of Plaintiffs and the Class Members.

269. Defendant has not satisfied its obligations and legal duties to Plaintiffs and the Class Members.

270. Green Diamond has claimed that it is taking some steps to increase its data security, but there is nothing to prevent Defendant from reversing these changes once it has weathered the

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

increased public attention resulting from this Breach, and to once again place profits above protection.

271. Plaintiffs, therefore, seek a declaration (1) that Green Diamond's existing security measures do not comply with its obligations and duties of care to provide adequate security, and (2) that to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Order Defendant to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and order Defendant to promptly correct any problems or issues detected by such third-party security auditors;
b. Order Defendant to significantly increase its spending on cybersecurity including systems and personnel;
c. Order Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;
d. Order Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
e. Order Defendant to segment Plaintiffs' and the Class's PII by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;
f. Order Defendant to cease storing unencrypted PII on its systems;
g. Order Defendant to conduct regular database scanning and securing checks;
h. Order Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

i. Order Defendant to implement and enforce adequate retention policies for PII, including destroying, in a reasonably secure manner, PII once it is no longer necessary for it to be retained; and

j. Order Defendant to meaningfully educate its current, former, and prospective employees about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all other similarly situated, pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. An order finding that Defendant engaged in the unlawful conduct as alleged herein;

c. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

d. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

e. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class, hereby demand a trial by jury on all appropriate issues raised in this Complaint.

Dated: July 1, 2024

By: */s/ Samuel J. Strauss*

Samuel J. Strauss (SBN 46971)
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com

William B. Federman (admitted *pro hac vice*)
Kennedy M. Brian (admitted *pro hac vice*)
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
E: wbf@federmanlaw.com
E: kpb@federmanlaw.com

Mason A. Barney*
Tyler J. Bean*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Telephone: (212) 532-1091
E: mbarney@sirillp.com
E: tbean@sirillp.com

Kaleigh N. Boyd, WSBA #52684
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
Telephone: (206) 682-5600
E: kboyd@tousley.com

**pro hac vice* request forthcoming

Counsel for Plaintiffs and the Putative Class

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com